UNIVERSITY OF BIRMINGHAM

Continuous Checking for Known Security Concerns

IRIS Security Workshop, 10th February, 2021

Mark Slater, Birmingham University

Introduction

Generally, announcements of security issues/vulnerabilities/compromises require checking some/all of the following:

- logs for suspect IPs/connections
- Particular files being present
- Variations in of particular package files
- Particular versions of packages

You can automate package updates to ensure any security patches are applied but the others are (too my knowledge at least!) not as easy to automate.

To get around this, I wrote a simple python script that performs the appropriate checks

The Script

The python script does the following:

Scan logs for suspect IPs

Looping over a list of logs (currently just /var/log/messages and /var/log/secure) it checks each line for a given list of IPs. Need to make sure this isn't being checked just after log rotation!

Checks if certain files are preset

Given a list of suspect files, go through and check if each one is present

Check if packages have been altered

Using 'rpm -V', validate if a list of packages (currently only openssh) have been altered. Note it ignores certain files (e.g. /etc/ssh/sshd_config) that would have been changed anyway

These checks are run once a day via a cronjob and any issues appended to a text file

Reporting on Errors

The script appends any issues to a simple text file stored in /root on the machine

Another script then checks this file (along with a few other things specific to Bham) every hour and reports it's results into the prometheus dropzone area

This is an option for the prometheus 'node_exporter' plugin that allows you to add in your own metrics:

```
--collector.textfile.directory=/var/lib/prometheus-dropzone
```

These are described using the following syntax:

```
bham_resources_intrusion_check{name="intrusion_check",environment="production"} 1
```

Alerts are setup in the prometheus instance that I check every day

General Points

This system is simple but gives me an extra layer of protection/early warning of any issues

It is also a lot easier to check for any new issues that are announced

I can be sure all machines I manage are being checked and have the latest checks in them thanks to the puppet infrastructure

The log checks would be a lot easier (and more thorough) done through Elastic Search but I haven't got an ELK stack at the moment